FIESTA: AN OPERATIONAL DECISION AID FOR SPACE NETWORK FAULT ISOLATION

Dawn Lowe (NASA/GSFC)
Bob Quillin (Stanford Telecommunications, Inc.)
Nadine Matteson (Stanford Telecommunications, Inc.)
Bill Wilkinson (Stanford Telecommunications, Inc.)
Steve Miksell (Stanford Telecommunications, Inc.)

Abstract

The Fault Isolation Expert System for Tracking and Data Relay Satellite System (TDRSS) Applications (FIESTA) is a fault detection and fault diagnosis expert system being developed as a decision aid to support operations in the Network Control Center (NCC) for NASA's Space Network. This paper presents the operational objectives which influenced FIESTA development and provides an overview of the architecture used to achieve these goals. The approach to the knowledge engineering effort and the methodology employed are also presented and illustrated with examples drawn from the FIESTA domain.

1.0 INTRODUCTION

This paper discusses the FAULT ISOLATION EXPERT SYSTEM for TDRSS APPLICATIONS (FIESTA). FIESTA is an expert system which is being developed to provide operator support in the Network Control Center (NCC) at Goddard Space Flight Center in the area of fault isolation.

Section 2 provides an overview of the Space Network and the role of the NCC. Section 3 describes the development environment established for FIESTA project effort.

Section 4 discusses operational concepts which have influenced the development and the displays which support these components. Section 5 presents an outline of the system architecture which supports the processing required to realize the operational concepts. Section 6 then describes the fault isolation methodology which FIESTA employs to provide the desired system capabilities focusing on knowledge engineering aspects of the FIESTA project.

2.0 SPACE NETWORK OVERVIEW

Figure 1 illustrates NASA's Space Network (SN) which combines space and ground segments to provide tracking and data acquisition services for spacecraft in near-Earth orbit (200 to 12000 km). The space segment of the baseline Space Network will consist of two operational geostationary satellites, Tracking and Data Relay Satellite East and West (TDRS-E and TDRS-W), as well as one spare satellite. From their geosynchronous orbit, the two operational satellites will be able to provide services to user spacecraft during 85 to 100 percent of their orbits. The TDR satellites are monitored and controlled from the White Sands Ground Terminal (WSGT), in White Sands, New Mexico. Collocated with WSGT is the NASA Ground Terminal (NGT), which provides the communications interface for the transfer of data from WSGT to the other Space Network elements and users, via the NASA Communications (NASCOM) network.

The Network Control Center (NCC) is the operations control facility for the entire Space Network. It serves as the focal point to network elements and user spacecraft facilities for coordination of all network support, and resolution of problems. The NCC's primary functions include scheduling network resources, equipment configuration direction, and service quality monitoring and assurance.

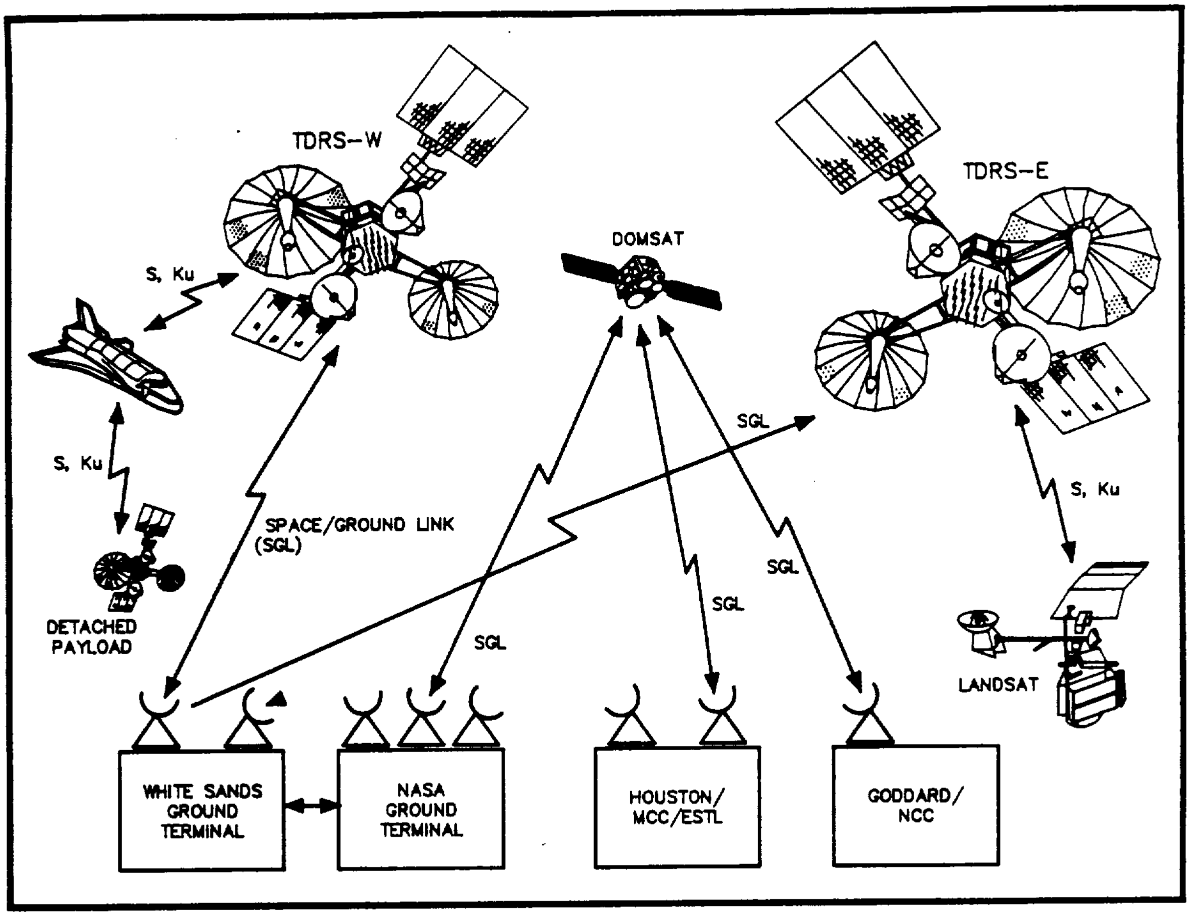

FIGURE 1: NASA SPACE NETWORK OVERVIEW

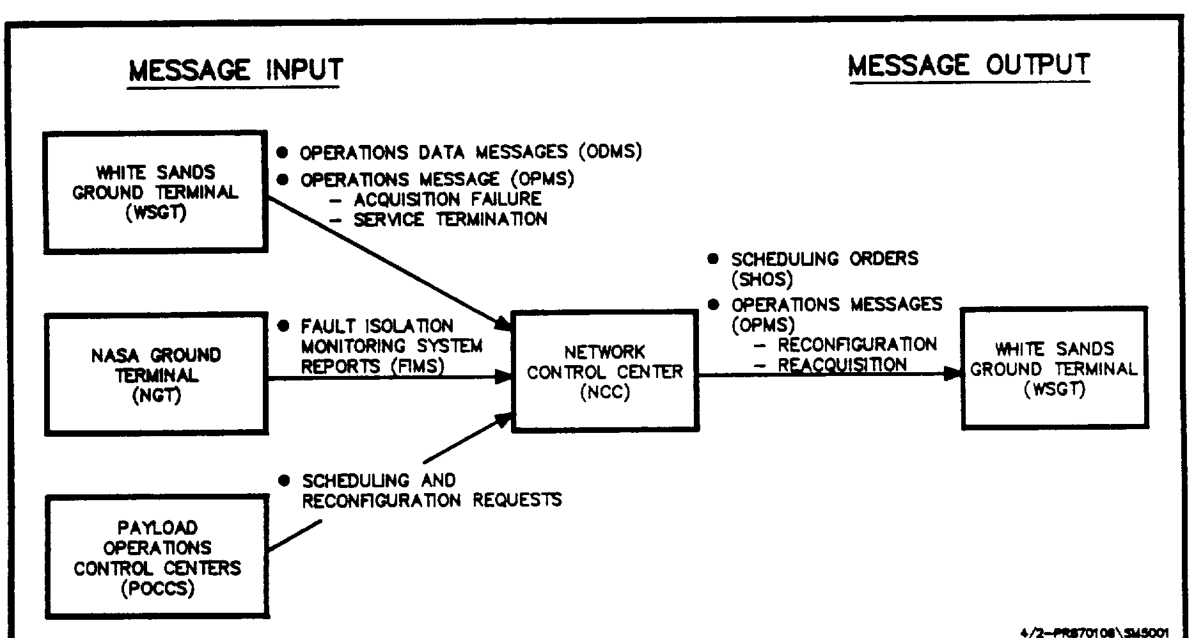

FIGURE 2: FIESTA DATA SOURCES

Role of the Network Control Center (NCC) in Problem Detection/Fault Isolation

Based on requests from user spacecraft control facilities, the NCC schedules "events", consisting of one or more services for a single user. Prior to the start of the event, Schedule Orders (SHOs) are transmitted by NCC to the network elements, indicating the start and stop time of each service, and specific configuration information. During real-time operations, NCC operations personnel monitor the status of network services to detect anomalies so that corrective action can be promptly initiated. The real-time nature of many user spacecraft operations, together with the high bandwidth data flow through the Space Network, combine to increase the critically of NCC's fault detection and isolation responsibilities. It is essential that problems are detected immediately, and service outages are resolved quickly, to minimize data loss and impact to the user mission. This function requires that NCC controllers and analysts continuously monitor network performance indicators, and compare expected versus actual values to detect anomalies. The NCC does not monitor user spacecraft telemetry, command, or tracking data directly. Rather, NCC receives network performance data (related to user services) in the form of high-speed electronic messages from the Space Network elements.

From WSGT, NCC receives Operations Data Messages (ODMs) every 5 seconds. These are generated by the Automatic Data Processing (ADP) equipment at WSGT, and indicate the status of all ongoing services through the TDRSS. They include such parameters as RF beam pointing angles, link status, signal strength, and bit error rate. At NGT, data quality monitoring is performed using Frame Analyzers. Data quality information produced by the Frame Analyzers is combined into Fault Isolation Monitoring System (FIMS) reports, which are sent to the NCC every 5 seconds. These messages include parameters such as frame sync lock status, and percentage of frames in lock. Figure 2 illustrates the additional high-speed message flow which is currently available to support NCC operations.

Currently, the contents of these messages are combined and presented on display screens to NCC operations personnel. Network Controllers and Performance Analysts monitor these displays, as well as ground control (reconfiguration) messages that alter the scheduled equipment configuration, to detect problems and determine appropriate courses of action. This task is an extremely labor intensive process. The quantity of information contained in the messages requires at least one (and in some cases two) display screens per service.

At the time of this writing, only one TDRS is operational, supporting a small number of user spacecraft. The Network Controllers and Network Performance Analysts are able to work together in teams to provide complete coverage of all ongoing services. However, they are reaching an information saturation point. When the second TDRS is launched, and the number of user spacecraft increases, the manual approach to network monitoring and fault detection/isolation will be inadequate. Some form of automation will be needed in order for the NCC to satisfy its mission-critical requirement to assure the quality and continuity of Space Network services. The purpose of FIESTA is to provide an intelligent assistant to the Space Network Controllers and Performance Analysts, that will continuously monitor selected services, detect faults, bring these faults to the attention of the controller/analyst, and isolate the source of a problem to the major system component level.

3.0 THE PROTOTYPE DEVELOPMENT ENVIRONMENT

The FIESTA prototype is currently being built in an off-line environment. This parallels conventional software development in which on-line validation occurs after off-line development and thorough system testing. The off-line development environment is made to look as much as possible like the NCC in terms of the data available and the software environment. A decision was made early to use a front end processor to isolate and simulate NCC interface functions. The benefit of this approach is that it separates the procedural interface functions from the knowledge-based functions that are the primary interests of the project.

High Speed Message (HSM) traffic from the Space Network is recorded at the NCC. These magnetic tapes provide "Automatically-obtainable situation data" (AOSD) used by the FIESTA standalone prototype. Data sources include actual missions as well as simulations run to create test data sets.

The FIESTA prototype consists of two computers and two bodies of software that communicate via commercially available networking tools. For the expert system component, the decision was made to use "off-the-shelf" hardware and a well supported expert system development shell. Such tools provide essential capabilities (e.g., an inference engine, a flexible data and knowledge representation language) and allow the development effort to be focused on the knowledge engineering task. Inference Corporation's Automated Reasoning Tool (ART) hosted on a Symbolics 3640 Lisp Machine was chosen. The FIESTA Front End Processor (FFEP) was prototyped on a VAX 11/730. The VAX was used for the sake of convenience and compatibility with other tools.

The NCC Simulator and AOSD Transformer

The FFEP software was christened "NSAT" for NCC Simulator and AOSD Transformer software. The NSAT was built to perform the following functions for the FIESTA prototype's development:

- To "simulate" the NCC insofar as providing AOSD to the rest of FIESTA,
- To isolate the expert system components from the preprocessing functions performed in the NSAT, the goals being to make the expert system component think it is fielded and to isolate NCC interface functions,
- To offload the Lisp Machine, translating coded HSM values to symbolic expressions amenable to use by the expert system application, and
- To provide a tool useful in development and testing of FIESTA - one for "feeding" the expert system components controlled amounts of data at controlled times; the programmer needs a tool to replay given scenarios to test and debug the expert system.

Figure 3 depicts the main components and data flows of the prototype. The prototype has been implemented in the STI development lab shown in Figure 4. The NSAT reads and translates AOSD from a disk file, transmitting it to the Lisp Machine under user control. A synchronizing Lisp Machine process reads AOSD over the net and does a bit of housekeeping. It makes the AOSD available in the Lisp world for the FIESTA process. (The Lisp Machine has only one address space so that global symbols can be used to pass arbitrary objects between Lisp Machine processes.) The FIESTA process then parses the AOSD and asserts it as a set of "facts" (one fact per service) into the ART database. When asserted as facts this data becomes available automatically to fault detection and diagnosis rules.

4.0 FIESTA OPERATOR/SYSTEM INTERFACE

The basic operational concept for FIESTA is to support NCC operations by automating network monitoring and fault detection as well as the reasoning process involved in fault isolation. To support these functions (monitoring, detection and isolation), an effective operator interface is required to allow FIESTA to serve as an intelligent decision aid.

This interface is provided by various types displays on a video terminal. Some information needs to be continuously and immediately available to the operator. This information includes the current services being monitored, their status, time of the latest message received, and an area for the display of alarm notifications. The current FIESTA system status and an operator options interface are also required. This information is grouped in a reserved area at the top of the screen. The space below is then free space, which the operators can customize with the displays of immediate interest. These five key windows are shown in Figure 5.

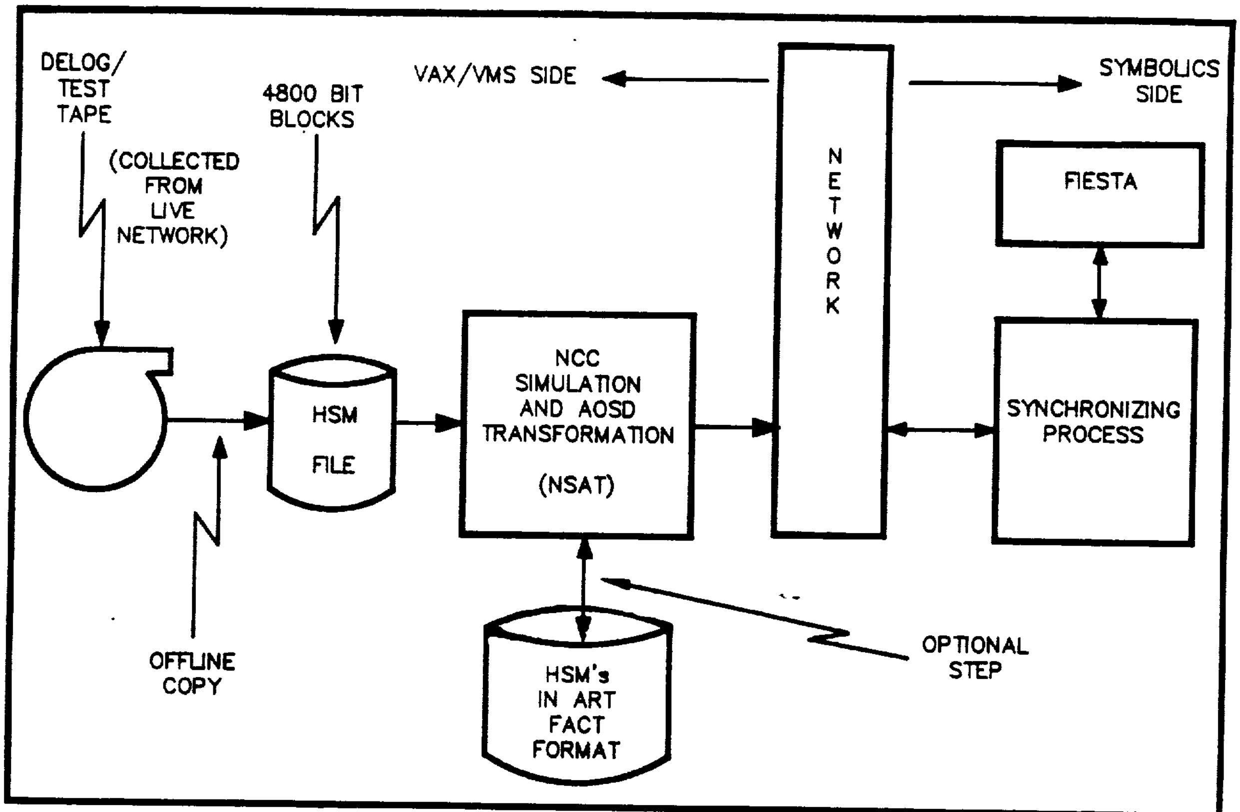

FIGURE 3: FIESTA TESTBED AUTOMATICALLY OBTAINABLE SITUATION DATA (AOSD) FLOW

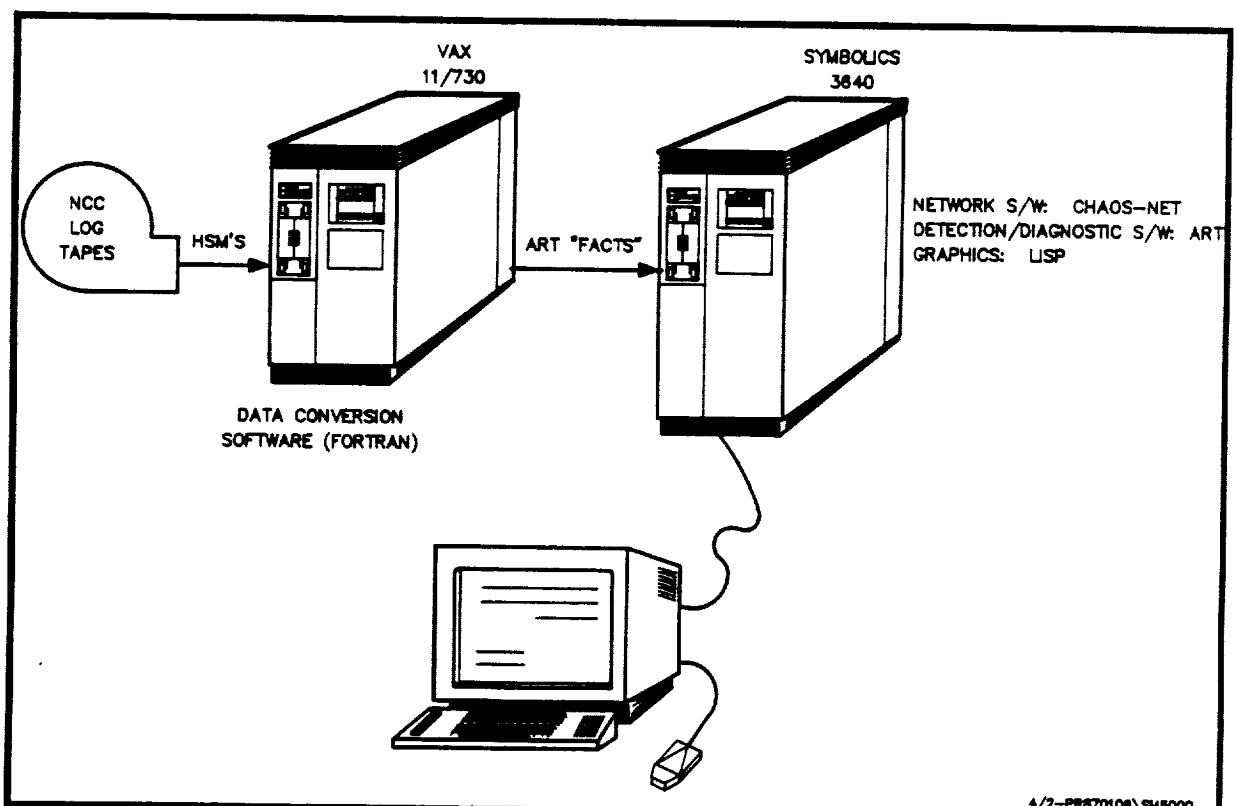

FIGURE 4: FIESTA PROTOTYPE (STANDALONE) CONFIGURATION

4.1 MONITORING DISPLAYS

Monitoring display are provided in several ways. The services window provides a high-level summary of the service status by reporting it as "acquiring", "nominal", "non-nominal", "transitional", or "late". A status of "acquiring" indicates that the link is in the process of being established, and dropouts should be expected. "Nominal" indicates that a good link has been established and all data looks good. "Non-nominal" signifies that bad data has been detected or that acquisition time is excessive. "Transitional" indicates that the service had been non-nominal, but now good data has returned. (to avoid treating rapid transient dropouts as separate faults a stabilization period is introduced before returning the status to nominal). Finally, "late" indicates that there are less than two minutes of scheduled service time remaining, a period when dropouts are common.

At a more detailed monitoring level, dynamic displays show relevant parameters in the high-speed messages. These are available as either cockpit or trending displays. Cockpit displays provide a "snapshot" of the most important parameter values and are automatically refreshed as new data arrives. The trending displays provide a history of parameter variation updating the graphs with additional information as messages are received. Figure 5 also provides example of each of these display types.

4.2 FAULT DETECTION DISPLAYS

In order to draw special attention to the occurence of significant fault related events, a notification window was implemented.

Whenever faults are detected or diagnoses are updated, a short message indicating the affected services and time of occurrence is posted. This is in addition to the summary status of non-nominal which will appear in the service window when a fault is detected.

4.3 FAULT ISOLATION DISPLAYS

When the notification is acknowledged by the operator, an explanation window is displayed. This window provides a description of the anomaly and the most likely diagnosis. The explanation window contains a justification option. When "justification" is selected, another window is opened which displays the evidence used in determining the conclusion shown. Both of these displays are shonw in Figure 6.

Additional diagnosis support is provided by the alternative hypotheses display. This display shows all the diagnostic alternatives currently under consideration and the positive and negative evidence for each. Further support as an intelligent decision aid is provided by the Recommended Action option. The recommended action window presents a series of alternative actions in order of probable usefulness.

The types of screens presented support the display requirements associated with the operational concept. Both operators and human factors engineers aided in the evaluation and evolution of the display concepts. Their involvement has contributed to a display system which is now ready for evaluation in an on-line environment.

5.0 ARCHITECTURAL OVERVIEW

The FIESTA Architecture was influenced by three critical elements. These were:

- The presence of independent data sources providing real-time situation data

- The requirements for supporting the operator interface to the system.

- The function of reasoning and inferencing which was central to the application.

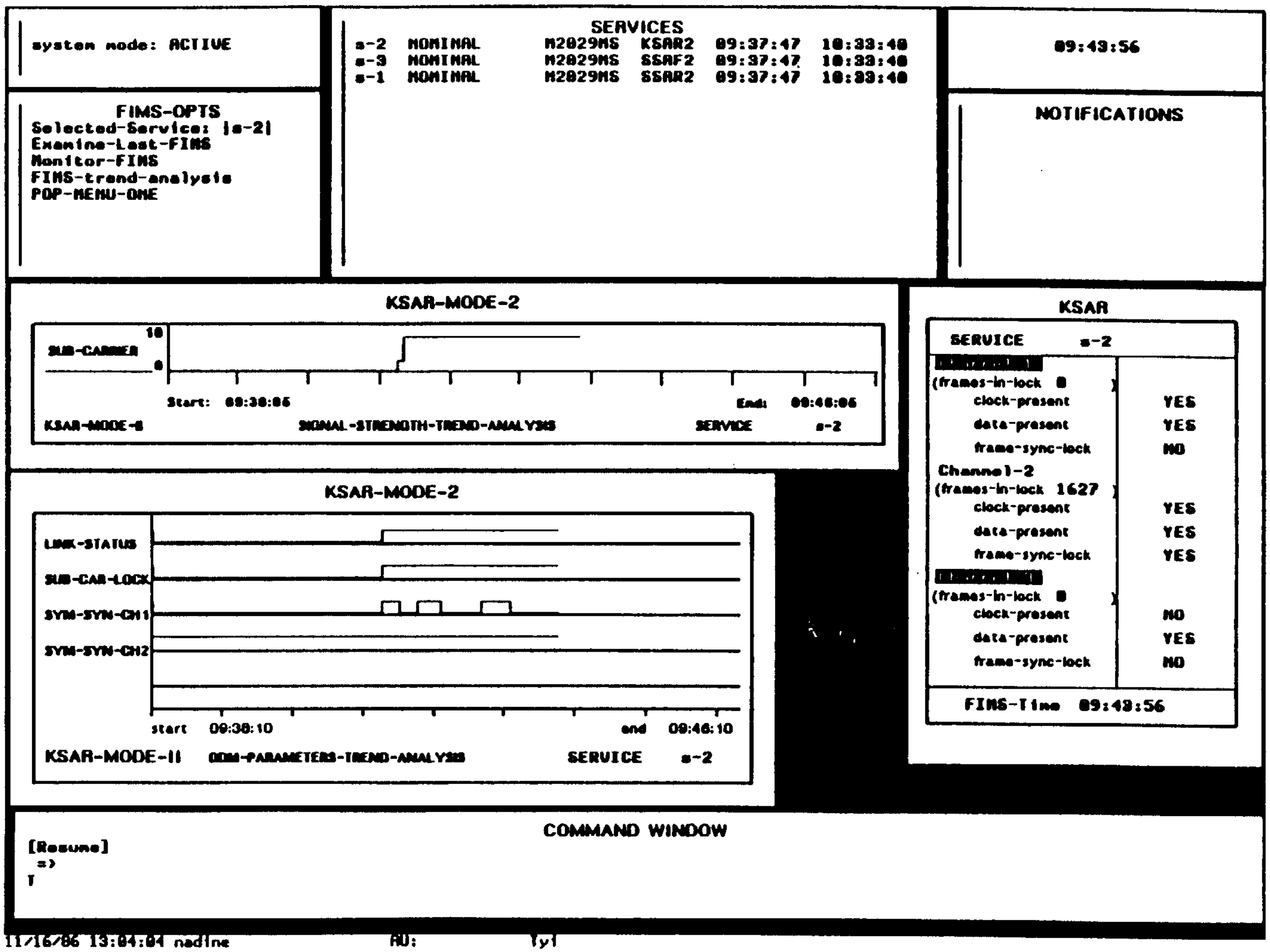

FIGURE 5: MONITORS AND DETECTION DISPLAYS

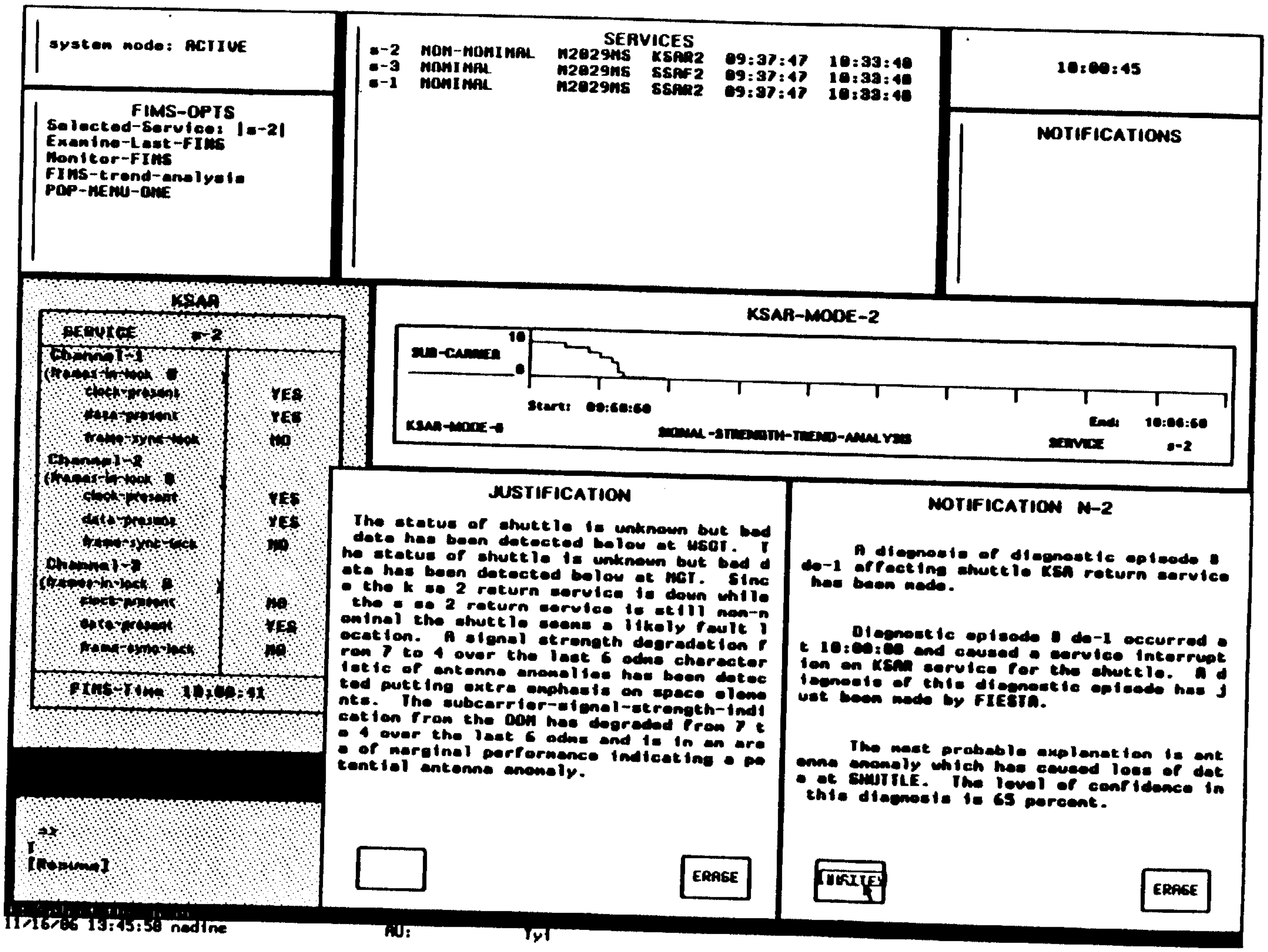

FIGURE 6: DIAGNOSTIC DISPLAYS

-12-

ORIGINAL PAGE IS OF POOR QUALITY

FIESTA rules ("productions") fall into three basic categories, corresponding to the major architectural design drivers. These are:

1) The front-end processor rules (interface to situation data);
2) The run-time monitor (interface to the operator); and
3) The expert system component (reasoning).

The expert/reasoning portion may be further subdivided into three parts (Kernel, Diagnostic and Assistant) reflecting specific fault reasoning functions performed by the system.

The FIESTA system architecture features three-way asynchronous operation of data handling, reasoning, and operator interaction to coordinate the elements involved. This asynchronous operation is accomplished by interfacing all components through a central knowledge base. Figure 9 provides an overview of the system architecture. The FIESTA front-end processor serves as a gateway for AOSD which is arriving from external data sources in real time. The FIESTA reasoning expert combines the situation data with its prestored knowledge base of rules, propositions, and frames to derive conclusions about the health of the system. Finally, the run-time monitor sends alerts and requested displays to the operator. It also enables the operator to request more information or enter any Manually Obtainable Situation Data (MOSD) that may be available. This data provides further information (via voice, special console, or hardcopy report) beyond that which is available automatically through high-speed message traffic.

The synchronization necessary to coordinate these components is provided by the fact database. The front-end processor, FIESTA expert, and run-time monitor consist of processes and rules which maintain and monitor this fact database. Activation of the rules is a data-driven function of the inference engine (provided by the ART package). Thus the processing of the inference engine addresses the problems associated with dealing with external data sources in real-time while simultaneously reasoning about the incoming data and responding to operator requests for data/advice (without overly restricting the timing of those requests). Figure 7 summarizes these architectural concepts, indicating the coordinating role played by the knowledge base and the groups of rules which provides the system capabilities.

6.0 METHODOLOGY

This section discusses the fault isolation methodology applied to the problem domain with an emphasis on how the application domain structure was mapped to a software design solution. The following elements comprise this domain structure:

- Operational Support Organization
- Acquisition Determination
- Fault Detection
- Fault Diagnosis
- Uncertainty Management

In designing and developing a knowledge-based system, it is extremely important to recognize and take advantage of the natural organization of this knowledge. The way the expert views and approaches the problem should drive the design of the system.

6.1 OPERATIONAL SUPPORT ORGANIZATION

Operational support at the Network Control Center is organized on a user spacecraft basis. For example, during Space Shuttle flights, a Shuttle operations team handles the Shuttle fault detection and diagnosis responsibilities at the NCC. With other users, a different set of operators is responsible for their support. Thus, operational specific knowledge has developed around each individual user spacecraft with a common base of general knowledge that is applicable to all users.

Real-time operations are organized on an event basis. An event is defined as a scheduled support period for one user spacecraft for one pass by the Tracking and Data Relay Satellite (TDRS). The event can be further broken down by services within that event. A service is defined

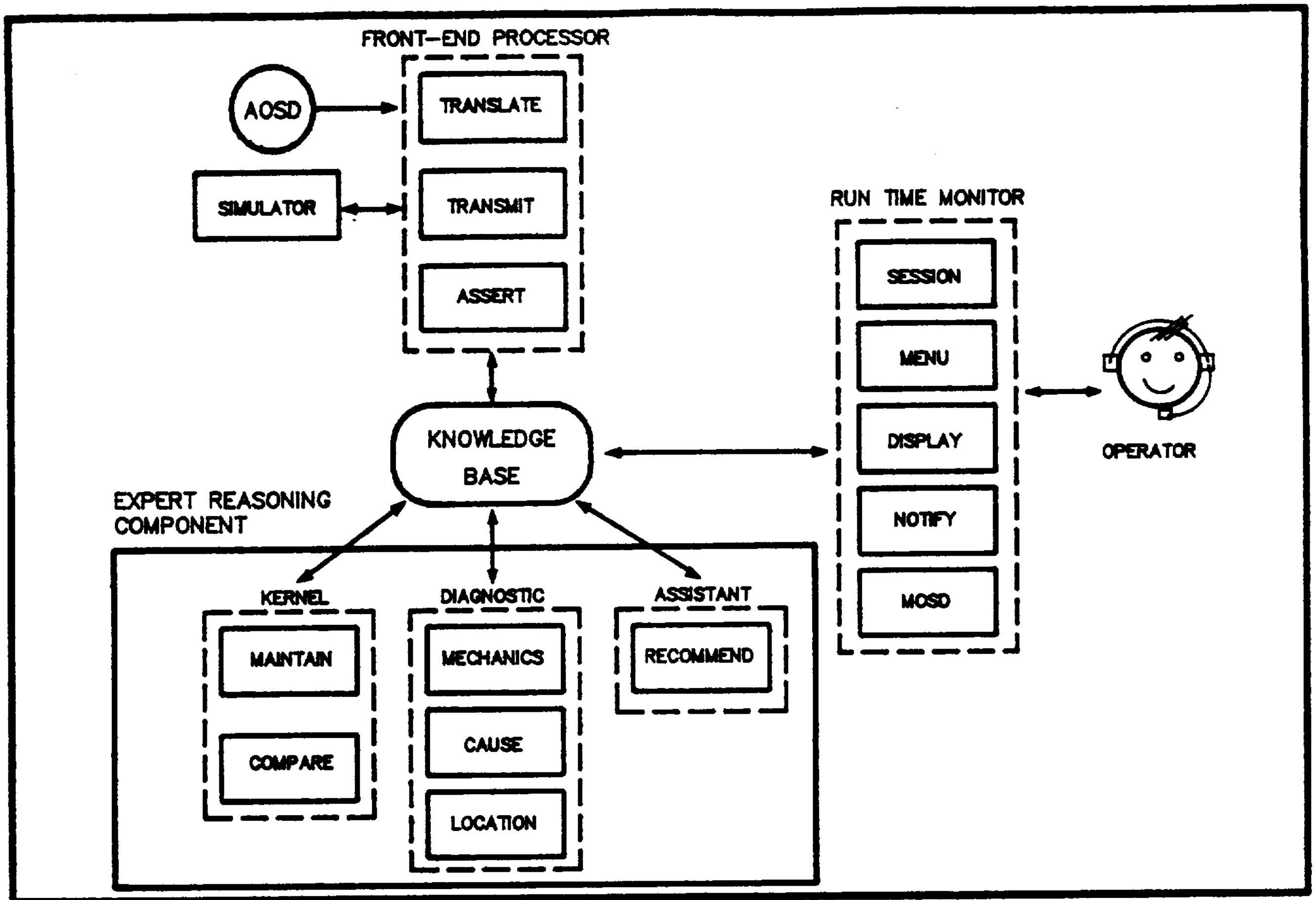

FIGURE 7: DETAILED FIESTA SYSTEM ARCHITECTURE

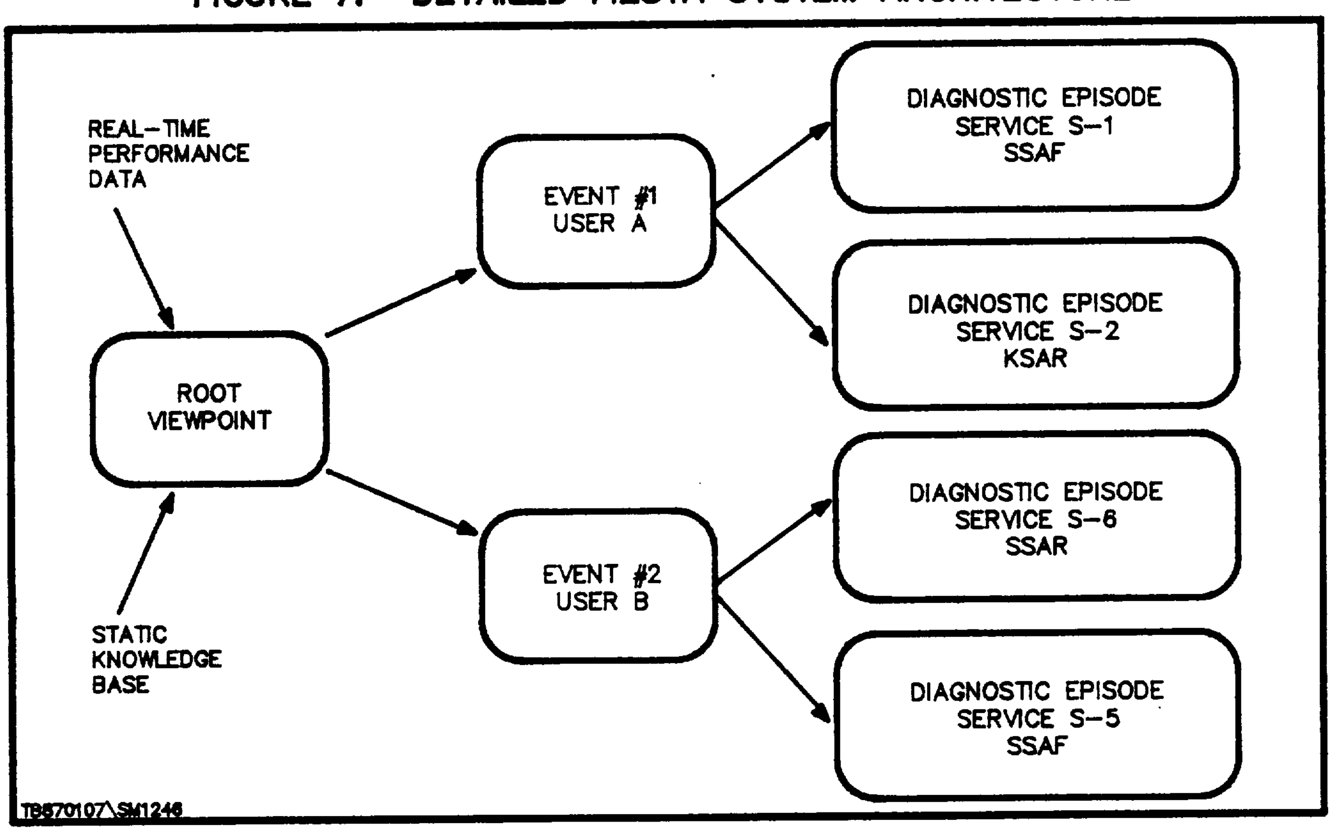

FIGURE 8: VIEWPOINT STRUCTURE

as a single communication link provided by the network (e.g., Ku-Band Single Access Return, or Multiple Access Return). All performance data received at the NCC is service specific, and thus faults are detected and diagnosed from a service perspective within the context of the event in which they occur.

Space Shuttle support was selected for this initial FIESTA prototype development. A Shuttle event consists of three services: S-Band Single Access Forward (SSAF), S-Band Single Access Return (SSAR), and Ku-Band Single Access Return (KSAR).

Figure 10 illustrates the type of data organization which was employed to separate generic Shuttle support knowledge from event-specific knowledge and event-specific knowledge from service-specific/fault-related knowledge. (The ART development package supports this tree-like organization, which includes inheritance, via its viewpoint mechanism. The nodes are referred to as viewpoints and this terminology will be employed).

The root viewpoint contains the static knowledge base (e.g., generic knowledge of the Space Network) as well as the dynamic situation data. The viewpoints sprouted off the root relate to separate user events currently monitored by the operator. Event-specific knowledge, such as appropriate nominal values and ranges, scheduled equipment chains, and event status and trends, reside in this viewpoint. The event viewpoints have access (through inheritance) to the background knowledge and situation data from the root viewpoint. All monitoring and real-time service support occurs in this event viewpoint.

When FIESTA detects an anomaly on a specific service, it sprouts a new viewpoint off the affected event node. This is termed a diagnostic episode. Detection of faults on other services will in turn result in new (diagnostic episode) viewpoints sprouted off the event node. This allows the system to independently reason about each diagnostic episode and also to share information among simultaneous diagnostic episodes (searching for commonalities) through the event viewpoint, where they share a mutual parent.

6.2 ACQUISITION DETERMINATION

The concept of acquisition plays a major role in FIESTA's diagnostic approach due to signal behavior differences before, during, and after acquisition. The normal event start time for the Shuttle precedes actual signal and data acquisition by several minutes. This implies that for the first several minutes of service the performance parameters will indicate the presence of no signal and no data. As the Shuttle comes into line-of-sight of the TDRS, the signal may behave erratically before finally locking up. Not until the signal exhibits steady signal-strength and demodulator-lock values will the operators consider service nominal. In addition, an important differentiation must be made between signal and data acquisition because:

- Signal acquisition can occur without data acquisition
- The Shuttle may schedule data on a channel for an entire event but only transmit on that channel for a portion of that event
- Positive signal acquisition without data acquisition points the problem to different diagnostic areas than combined negative signal and data acquisition.

The FIESTA design had to account for these operational characteristics to recognize that Shuttle services routinely lock up late, that erratic behavior can be expected during acquisition, and that acquisition is a two-step process (signal and data).

Immediately following event startup, FIESTA tracks the status of all signal-related performance parameters for the return services. When these parameters have remained nominal for two consecutive minutes on a particular service, FIESTA determines acquisition is complete and will begin to monitor the service for ensuing anomalies. Any signal-related out-of-range or out-of-tolerance conditions that are detected will no longer be considered acquisition idiosyncrasies but actual faults. At this point FIESTA changes the status of the service from "ACQUIRING" to "NOMINAL" both internally and externally (notifying the user). Data acquisition is handled similarly through monitoring of appropriate bit/symbol-sync lock and frame-sync lock parameters.

6.3 FAULT DETECTION

On the surface, fault detection seems trivial: identify anomalous conditions through the monitoring of performance parameters or through user notification and initiate the fault diagnosis process. Upon closer inspection, the problem becomes more complex and logic-based than one would first expect. Before operators can recognize an out-of-tolerance or out-of-range condition, they must first identify (albeit subconsciously) the nominal value or range that is exceeded. For example, nominal signal strength range will vary among users and allocated equipment chains. Operators also routinely ignore apparent signal or data dropouts caused by service configurations, reconfigurations, and service-to-service handovers. The ability to differentiate seemingly anomalous behavior from actual anomalous behavior is an expert capability that is easily overlooked. FIESTA anticipates the majority of these types of conditions and does not open up diagnostic episodes for expected service dropouts. This capability proves to be extremely important for system performance considerations to avoid paying unnecessary diagnostic processing penalties and to minimize false alarms.

Fault detection rules provide an independent source of network status information to the diagnostic rules. Diagnostic rules rely on this network status data to reason about current conditions. The detection rules monitor for anomalous conditions, detect non-nominal parameters and initiate diagnostic episodes based on detected conditions, continue to monitor and provide network status information to the diagnostic rules through a diagnostic episode, and determine when the diagnostic episode can be terminated.

6.4 FAULT DIAGNOSIS

To model the fault diagnosis process, the FIESTA design tried to parallel the thought patterns of the experts by selecting the most likely fault from a pool of known possibilities. While experts often arrive at the solution immediately, the subconscious steps they took to get there will comprise the diagnostic methodology FIESTA needs to follow. The model developed involves hypothesizing all known fault causes and fault locations (at a high level), immediately ruling out some or most, and pursuing others to a lower level of detail. This hierarchical fault cause/location model utilizes a hypothetical reasoning structure to rank the possibilities and present the most likely pair.

The highest level hierarchical breakdown occurs between fault location and fault cause. Both of these branches provide significant information on fault conditions in the network. The two branches can be viewed as two independent experts, a fault location expert who determines the point at which data was lost and a fault cause expert who explains why. After their analysis, the two experts confer and present the most likely fault location and cause to provide a twofold explanation of the anomaly.

Utilizing the natural hierarchy of TDRSS Network fault causes and fault locations provides FIESTA with the flexibility to diagnose locations and causes in as much detail as possible. In some cases, the available data may not be sufficient to pin down a specific piece of equipment or a particular network operator, but the data may be sufficient to isolate the location to a network element (e.g., a specific ground terminal), set of elements (e.g., either the Shuttle or the relay satellite), or isolate the cause to an operational type of error at a high level.

Hence, this structure attempts to give the diagnosis as much flexibility and depth to accommodate varying levels of operator experience and skill and to adapt to a variety of data availability conditions.

6.5 UNCERTAINTY MANAGEMENT

A fundamental design characteristic of an expert system is its uncertainty management approach. The inferences humans make are often uncertain; certain conditions may "suggest," "sometimes result in," or "may mean" a corresponding conclusion. Thus, a mechanism must be developed to:

- Represent probabilistic statements;
- Gather and combine evidence for and/or against a certain hypothesis; and
- Present this hypothesis and its "certainty" to the user.

Various alternatives exist for representation of uncertainty (Dempster-Shafer Theory of Evidence, fuzzy logic, Bayesian inference). The technique chosen for FIESTA was the MYCIN CF Model [1].

The following reasons form the basis for our choice of the CF Model: (1) the MYCIN CF Model is a standard in the field in that it has withstood the test of time, scrutiny, and numerous implementations outside of its original application; (2) the MYCIN domain was diagnostic as is FIESTA's -- FIESTA monitors incoming symptoms (network performance data), detects and diagnoses the problem and acts as an operational consultant; and (3) this model is easily implementable via LISP and ART code. Another feature we have found through our prototyping efforts is that the CF Model is easily understandable and integrates well into the operational psyche of its intended user community.

---

[1] Buchanan, B. G., and Shortcliff, E. M., 1984. Rule-Based Expert System: The MYCIN Experiments of the Stanford Heuristic Programming Project, Reading, Mass., Addison-Wesley.

Summary

This paper has presented some highlights of the expert system FIESTA and the knowledge engineering effort which has supported its development. FIESTA is targeted for on-line deployment in the NCC. Current development efforts are focused on the transition from its current standalone prototype mode to that of an on-line test bed environment. Issues of real-time data acquisition and real-time performance of the demonstrated capabilities are currently being addressed. These capabilities support the operational concepts of automation and provide an illustration of how expert system methodology can expand automation concepts to include reasoning and decision aid support.

ACKNOWLEDGMENTS

FIESTA development has been undertaken by Stanford Telecommunications, Inc. as a subcontractor to the Bendix Field Engineering Corporation (BFEC). Project support has been provided by the National Aeronautics and Space Administration under Contract #NAS5-27600.

The overall support and encouragement of Paul Ondrus and Anthony Maione of NASA/GSFC are particularly appreciated and acknowledged. The knowledge engineering effort was fortunate to have the operational expertise and cooperation of Joe St. John and Bill Webb of BFEC. Testing materials and network insights which have proved invaluable in development efforts have been provided both directly and indirectly by Tom Gitlin (BFEC). The administrative and logistics efforts of Hugh Bath (BFEC) and his technical staff were most supportive.

Portions of this paper have been drawn from the article "Expert System Fault Isolation in a Satellite Communication Network" prepared for inclusion in the book EXPERT SYSTEM APPLICATIONS TO TELECOMMUNICATIONS, J. Liebowitz, ed. to be published by John Wiley and Sons, Inc. (tentatively 1987).